AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

Southern District of Texas

United States of America
v.
JASON DEL MULDER

Case No. **4:20mj2434**

Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of Sept. 12, 2020 to Nov. 11, 2020 in the county of Harris in the Southern District of Texas, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C. § 2252A(a)(2)(B)	Receipt of materials constituting or containing child pornography.

This criminal complaint is based on these facts:

See attached Affidavit

☑ Continued on the attached sheet.

Complainant's signature

Cecil Arnold, Detective
Printed name and title

Sworn to before me telephonically.

Date: 12/01/2020

Judge's signature

City and state: Houston, Texas

Sam S. Sheldon
Printed name and title

AFFIDAVIT IN SUPPORT OF A CRIMINAL COMPLAINT

I, Cecil Arnold, being duly sworn, hereby depose and state the following:

1. I am peace officer, certified by the State of Texas by way of the Texas Commission on Law Enforcement (TCOLE) and currently employed as a Detective with the Pearland Police Department assigned to the Criminal Investigations Division. Affiant, Cecil Arnold, has been a law enforcement officer since November of 1998. Affiant is currently assigned to the Internet Crimes Against Children Task Force, where his duties include the investigation of Child Pornography, Child Sexual Assault, and Child Sexual Exploitation. Affiant is also assigned to the ICAC (Internet Crimes Against Children) Taskforce for the Houston Metro area. The Houston Metro Internet Crimes Against Children Taskforce is a federally funded group of Local, State, and Federal Law Enforcement Officers who received specialized training in the area of digital child exploitation and are tasked for investigations related to those crimes.

2. I have received extensive training in the area of child exploitation and child pornography. I have also discussed the subject matter with other experienced SA's and Law Enforcement Officers (LEO's), as well as interviewed several juvenile victims and defendants regarding the matter. I have also had the opportunity to observe and review numerous examples of child pornography in all forms of media, to include computer media.

3. Child Pornography, as defined in Title 18 U.S.C. § 2256, is:

"any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where – (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; . . . [or] (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct." For conduct occurring after April 30, 2003, the definition also includes "(B) such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from that of a minor engaging in sexually explicit conduct."

4. This Affidavit is made in support of a criminal complaint charging Jason Del Mulder with violating Title 18 U.S.C. § 2252A(a)(2)(B), the receipt of child pornography.

5. This Affidavit is being submitted for the limited purpose of securing a criminal complaint, I have not included each and every fact known to me concerning this investigation, I have set forth only those facts I believe are necessary to establish probable cause that evidence of violation of 18 U.S.C. § 2252A(a)(2)(B), receipt of child pornography, that occurred between the dates of September 12, 2020 and November 11, 2020; were committed by Jason Del Mulder. Throughout this Affidavit, statements made by sources of information and other witnesses are set forth in substance and in pertinent part unless otherwise indicated. Further, the facts and circumstances of this investigation have been set forth in pertinent part for the purpose of this Affidavit and do not include the complete factual history of this investigation, or all of its details.

6. Affiant is aware from training and experience that a Network exists, hereafter referred to as "The Network" that allows users to share and obtain child pornography. Affiant knows from his training, experience, and conversations with other Law Enforcement Officers that computer users can install publicly available software that accesses The Network to obtain child pornography. The actual name of The Network is known to law enforcement. The Network remains active and disclosure of the name of The Network would potentially alert The Network's users to the fact that law enforcement action is being taken against The Network, possibly provoking users to notify other users of law enforcement action, flee, and/or destroy evidence. Accordingly, for purposes of the confidentiality and integrity of the ongoing investigation involved in this matter, specific names and other identifying factors have been replaced with generic terms and The Network will be identified as "The Network."

7. Affiant knows that The Network is a distributed, Internet based, peer-to-peer Network which attempts to let a user anonymously share files and chat on forums. The Network is free software and the source code is publicly available. Communications between computers running The Network, or nodes, are encrypted and routed through other Network nodes making it difficult to determine who is requesting the information and what the content is of the information being requested. Affiant knows from his training, experience, and conversations with other Law Enforcement Officers that The Network

provides a platform for message forums and websites only available through The Network.

Factual Basis to Support Criminal Complaint

8. On Tuesday, September 22, 2020, while reviewing data received by law enforcement Network computers, I observed IP address 70.241.112.245, with the Network Location ID 0.499186487767195, requesting blocks of suspected child pornography files. While it is not an absolute certainty the user was the original requestor, with respect to each file, considering the number of requested blocks, the total number of blocks required to assemble the file, and the number of peers the user had, the number of requests for blocks of the file is significantly more than one would expect to see if the user of IP address 70.241.112.245 were merely routing the request of another user.

Between Saturday, September 12, 2020 at 9:51 PM UTC and Sunday, September 13, 2020 at 12:29 AM UTC, I learned a computer running Network software with an IP address of 70.241.112.245, with an average of 43.6 peers, requested from a law enforcement computer 8,145 required pieces needed to assemble a file with a SHA1 digital hash value of OVLTRUD5WZASBC2QEJRUWNFFVDX7HPUM, of which 137 were available on the law enforcement computer. This file can be downloaded from The Network using the specific key known to law enforcement which is publicly available. This key contains the images represented by the above digital hash value.

9. Between Saturday, September 12, 2020 at 10:19 PM UTC and Sunday, September 13, 2020 at 12:04 AM UTC, I learned a computer running Network software with an IP address of 70.241.112.245, with an average of 49.9 peers, requested from a law enforcement computer 1,537 required pieces needed to assemble a file with a SHA1 digital hash value of 6AGEPH44E54J7LSIEXUQY6GQXAUFFB2X, of which 26 were available on the law enforcement computer. This file can be downloaded from The Network using the specific key known to law enforcement which is publicly available. This key contains the images represented by the above digital hash value.

I learned between Saturday, September 12, 2020 at 10:46 PM UTC and Sunday, September 13, 2020 at 12:15 AM UTC, I learned a computer running Network software with an IP address of 70.241.112.245, with an average of 50.5 peers, requested from a law enforcement computer1,842 required pieces needed to assemble a file with a SHA1 digital hash value of YFOVWWTA2TY2GP7447A6JJLCMNXDCT53, of which 36 were available on the law enforcement computer. This file can be downloaded from The Network using the specific key known to law enforcement which is publicly available. This key contains the images represented by the above digital hash value.

10. On Tuesday, September 22, 2020, I checked the IP address 70.241.112.245 through Maxmind`s database of IP addresses. Maxmind indicated that the IP address provided is believed to be used in the Friendswood, TX area.

I utilized the undercover software`s database where he learned that I.P. address 70.241.112.245 had been observed to be attempting to receive image and video files depicting known child pornography from September 12, 2020 until September 13, 2020, amounting to many unique pornographic images depicting children engaging in sexual acts. Based on a review of those requests I believe that the user of the IP address of IP 70.241.112.245 was the original requestor of the files described below.

11. I began to investigate the location of the user requesting the above-mentioned files. From training and experience, I know that I.P. addresses are assigned by the governing body of the internet to service providers for the use by their customers in connecting to the internet. Additionally, I know from my training and experience that there is a master list of I.P. addresses maintained by the American Registry of Internet Numbers (ARIN). I conducted a search through ARIN to locate the assigned owner of the I.P. address, 70.241.112.245 from which videos/images of child pornography were being sent or requested; where I learned that the I.P. addresses are owned by AT&T Internet Services.

12. On September 22, 2020, I contacted Special Agent Dewayne Lewis (Homeland Security), whom affiant knows to be credible and reliable, and a fellow task force member. Special Agent Lewis issued an administrative subpoena to AT&T Internet Services requesting

subscriber information for I.P. address 70.241.112.245 on the listed dates and times above, requesting subscriber information.

On September 23,2020 AT&T responded to the subpoena request and stated that the above mentioned I.P. address returned to:

Kenneth Copley
2738 Safe Harbor Circle
Friendswood, Texas 77546

13. I reviewed the list of files that I.P. address 70.241.112.245 was trying to obtain. I attempted to download three of the files from The Network using the same keys that IP Address 70.241.112.245 used, and I was successful in obtaining all three of the said files from the Network on September 22, 2020. Three of the files I observed are considered to be child pornography under the laws of the United States.

The first key contained a zip file of 57 child pornography videos. The videos appear to be of the same naked prepubescent juvenile who is approx. 3 years of age. In these videos an adult male is inserting his erect penis into the child`s vagina and anus. The child is also depicted inserting her hand into an adult female`s vagina.

The second key contained a video that is 1:55 seconds in length and depicted a naked prepubescent juvenile male approx. 5-6 year of age. In the video the juvenile male is performing oral sex on an adult male. The adult male inserts his erect penis into the child`s anus.

The third key contained a video that is 4 minutes and 22 seconds in length. This video depicts a naked juvenile male approx. 8-10 years of age. In the video the juvenile male is inserting his finger into his anus and masturbating.

14. On November 11, 2020, I along with other members of the Houston Metro Internet Crimes Agaisnt Children task force executed a state search warrant, obtained based on the information above, at 2738 Safe Harbor Circle in Friendswood. I made contact with Kenneth Copley at

the front door and advised him of the search warrant. Once the home was secured, I conducted recorded interviews with the residents.

All residents denied any knowledge of The Network program or viewing any child pornography. Information gathered during the interviews with the residents indicated that a friend named Jason Mulder comes over on the weekends to play computer games and uses their Internet connection. The residents stated that Jason Mulder is a registered sex offender who has been to prison for possession of child pornography and lives in a hotel off Fuqua.

15. I then spoke with Det. Cox and Det. Staton, with the Pearland Police, who are certified computer forensic examiners. They stated that they processed the electronic devices in the home and did not locate any Network programs on the computers or any child pornography.

I checked the sex offender data base and was able to corroborate the information that I had learned from speaking with the residents. Jason Mulder is a registered sex offender who lives at an extended stay hotel off Fuqua in Houston, 12485 Gulf Freeway, Houston, TX 77034. I drove to that location and spoke with the manager who confirmed that Jason Mulder does live there in a particular room, number which was given to law enforcement. Later in the day Det. Nettles, with the Webster Police Department, and fellow task force member, conducted a knock and talk at Mr. Mulder`s hotel room.

16. During the recorded knock and talk with Det. Nettles he obtained consent from Mr. Mulder to check his laptop. I spoke with Det. Staton who checked Mr. Mulder`s laptop at the hotel room. Det. Staton told me that he located information that this laptop did have The Network on it and was last on the Network about a week ago. Det. Staton stated that he located link files to possible child pornography titles being downloaded from The Network. Det. Staton stated that Mr. Mulder has been using C-Cleaner to erase what is being done on this laptop.

The laptop was seized in order to obtain a state search warrant.

17. On November 13, 2020, I completed the state search warrant to process Mr. Mulder's laptop which was signed by Harris County District Judge Luong.

Forensic analysis performed by Det. Cox on the laptop revealed that Jason Mulder has been running anti forensic software such as C-Cleaner on his computer regularly. He stated that he is not able to recover any videos or pictures that have been downloaded or viewed. Det. Cox was able to see that the Network was installed and deleted numerous times on this computer. Det. Cox stated that he was able to recover file titles that indicate that these were child pornography files that had been downloaded via The Network. Some of those titles were "4yo cum in ass", "baby fucked", "child love" and "my fucking pedo day".

Det. Cox was able to locate the file title babyshi%20near%20complete.7z. This title was located in Mr. Mulder`s download section of his Network folder showing that it had been downloaded on September 12, 2020. This video is one of the three child pornography files listed above. Det. Cox was also able to show that this computer was using the IP address at the hotel to access The Network and download titles indicative of child pornography.

18. On November 23, 2020, I received a phone message from Jason Mulder asking me to give him a call. In the message Jason Mulder stated that it had been 10 days since his computer was taken and he wanted to know when he was going to get it back. I returned Mr. Mulder`s phone call and spoke with him on a recorded phone line. The following is a synopsis of our recorded conversation. Mr. Mulder initially wanted to know when he was going to get his computer back. As the conversation continued, I informed Mr. Mulder what I had learned from Det. Cox concerning his computer. It was at this time that Mr. Mulder broke down and provided me with the following information.

Mr. Mulder stated that he fell off the wagon and had been using The Network to download and view child pornography. He stated that he first learned about The Network while in prison and when he got out began to use it. He stated that he would go to the freesites and gather the keys that would download child pornography. He stated that after he downloaded and viewed the videos, he would get very upset with what he had done and would delete the videos and un-install The Network program from his laptop and run C-Cleaner. He stated that he wants to stop what he is doing and needs additional help.

Mr. Mulder stated that the residents of the home where the first state search warrant executed had nothing to do with child pornography and he is very upset with himself for getting them

involved in his problems. He stated that the reason it was tied to their IP address was because prior to leaving his room at the hotel he had been downloading child pornography but had not completed the download. He stated that when he connected to the network at the residence his computer continued downloading the child pornography. He stated that is why the IP address returned to the resident's home.

Conclusion

19. Based on the information set forth above, your Affiant believes there is probable cause to believe that between the dates of September 12, 2020 and November 11, 2020, Jason Del Mulder was in violation of Title 18 U.S.C. § 2252A(a)(2)(B) by receiving child pornography.

Cecil Arnold
Detective
Pearland Police Department

Subscribed and Sworn to telephonically on December 1, 2020 and I find probable cause.

Sam S. Sheldon
United States Magistrate Judge
Southern District of Texas